

Application No.: 10/526,206

Docket No.: 09669/054001

REMARKS

Please reconsider the application in view of the above amendments and the following remarks. Applicant thanks the Examiner for carefully considering this application.

Disposition of claims

Claims 1, 2, and 4-7 were pending in this application¹. Claims 2, 4 and 6 have been cancelled without disclaimer or prejudice. Thus, claims 1, 5, and 7 are now pending in this application. Claims 1, 5, and 7 are independent.

Claim amendments

Claims 1, 5, and 7 have been amended by way of this reply to further clarify the claimed invention. Support for the amendments may be found, for example, in paragraph [0033] of the publication of the Specification (*see* US 2006/0041568). No new matter has been added by the aforementioned amendments.

Rejections under 35 U.S.C. § 102

Claims 1 – 7², stand rejected under 35 U.S.C. § 102 (e) as being anticipated by WO 02/054663 (hereinafter “Quick”). Claims 2, 4, and 6 have been cancelled by this reply. Accordingly, this rejection is now moot with respect to the cancelled claims. To the extent that this rejection still applies to the remaining amended claims, the rejection is respectfully traversed.

¹ Applicant notes that claim 3 was cancelled by the previous response.

² Applicant notes that claim 3 was cancelled by the previous response. Accordingly, Applicant has responded to the rejection on this basis.

Application No.: 10/526,206

Docket No.: 09669/054001

The remaining amended claims have been amended to clarify that: (i) the message to be hashed includes a key and public data in a specific sequence (*see e.g.*, Published Specification, [0008]); (ii) when the key proceeds the public data: the key is hashed by the smart card to generate a hashed key and then the hashing function is applied, in the communication device, to the hashed key along with the public data (not hashed) to generate the hashed message (*see e.g.*, Published Specification, [0033] and Fig. 4); and (iii) when the public data proceeds the key: the public data is hashed by the communication device to generate hashed public data and then the hashing function is applied, in the smart card, to the hashed public data along with the key (not hashed) to generate the hashed message (*see e.g.*, Published Specification, [0033] and Fig. 3). Thus the order of applying the hash functions changes depending on the message to be hashed.

Turning to the rejection, for anticipation under 35 U.S.C. § 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present (See M.P.E.P. § 2131). From the above discussion and the reasons set forth below, Applicant believes that Quick fails to show or disclose all the limitations of the amended independent claims.

Specifically, Quick is directed to a method and system for authenticating a subscriber outside their home system. *See* Quick, Abstract. In order to authenticate the subscriber, Quick discloses a method for generating and verify a primary signature. *See* Quick, FIG. 3. In order for such a system to work, the steps used to generate the signature must be performed in the same manner each time such that the generated signature (370 in FIG. 3) may be verified. In contrast, the amended independent claims describe a method, apparatus, and system in which the steps used to generate the hashed message vary based on the message to be hashed. In particular, the order in

Application No.: 10/526,206

Docket No.: 09669/054001

which the steps are performed to generate the hashed message is dependent upon whether the key proceeds the public data or vice versa.

Applicant respectfully asserts that the steps performed in the signature generation disclosed in Quick are always performed in the same order and that there is not indication that input used in one or more of the steps disclosed in Quick alter the subsequent order of the steps used to generate the signature. In view of this, it logically follows that Quick does not disclose the generation of a hashed message, where the steps used to generate the hashed message vary based on the sequence of the data within the message.

In view of the above, amended independent claims 1, 5, and 7 are patentable over Quick. Accordingly, withdrawal of this rejection is respectfully requested.

Application No.: 10/526,206


Docket No.: 09669/054001

Conclusion

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 09669/054001).

Dated: October 31, 2007

Respectfully submitted,

By  # 20031 ALY DASSA
Jonathan P. Osha
Registration No.: 33,986
OSHA · LIANG LLP
1221 McKinney St., Suite 2800
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Applicant

288565_1